Intermediate Math Circles
Wednesday November 23 2016
Modular Arithmetic II

1 Introduction

Welcome back! In this seminar we will apply our knowledge of modular arithmetic to:

- Fermat's Little Theorem and
- security problems.

2 Recall

For any a and b in $\mathbb{Z}$ with $b > 0$ there exists $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ with $0 \leq r < b$ such that

$$a = bq + r.$$

Here, q is called the quotient when a is divided by b and r is the remainder when a is divided by b. Note that b divides a exactly when the remainder when a is divided by b is 0. In fact, q and r are unique (i.e. the only numbers which satisfy this property).

Definition 1. *Let m be a positive integer. Let a and b be integers. We say that a and b are congruent modulo m, written $a \equiv b \pmod{m}$, if a and b have the same remainder when divided by m.*

So what does it really mean to say $a \equiv b \pmod{m}$? Well, it means that

$$a = mq_1 + r,$$

for some $q_1 \in \mathbb{Z}$ and integer r such that $0 \leq r < m$. Moreover,

$$b = mq_2 + r,$$

for some $q_1 \in \mathbb{Z}$. Note that the q_i's may be different but the r's are the same!!! Basically, a and b are congruent modulo m if they "look the same up to a multiple of m"!

Properties. *Let m be a positive integer and let $a, b, a', b', c \in \mathbb{Z}$. Then*

1. *If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $a + b \equiv a' + b' \pmod{m}$ and $ab \equiv a'b' \pmod{m}$.*
2. *If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.*
3. *if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.*
4. *$a \equiv a \pmod{m}$ for every $a \in \mathbb{Z}$.*
5. *$a \equiv 0 \pmod{m}$ exactly when m divides a.*
6. *If $a \equiv r \pmod{m}$ with $0 \leq r < m$ then r is actually the remainder when a is divided by m.*

THE PUNCHLINE: Given a positive integer m, working modulo m, you can reduce any integer n by adding or subtracting multiples of m until you get some number r such that $0 \leq r < m$. This r that you find is actually the remainder when n is divided by m.

BREAK FOR PROBLEM SET

3 Fermat's Little Theorem

Pierre de Fermat is a famous French mathematician who had made numerous contributions to calculus and number theory. One of his most famous results is his "little theorem". Dated in a 1640 letter by Fermat himself, the result says:

Theorem 1 (Fermat's Little Theorem)**.** *If a is an integer and p is a prime number then*

$$a^p \equiv a \pmod{p}.$$

Otherwise stated, $a^p - a$ is always a multiple of p. Recall that by a prime number we mean a positive integer $p > 1$ such that the only positive divisors of p are 1 and p itself. For instance, 2,3,5,7,11,13 are all prime numbers while 4,6,8,9,10,12 are not. Positive integers which are not prime are called composite.

Last time you were asked in a true/false question whether or not the following statement was true:

$$\text{If } a|(bc) \text{ then } a|b \text{ or } a|c.$$

You were successful in saying this statement is false! For instance, $4|(2 \times 2)$ by $4 \not| 2$. However, prime numbers have a special property which makes the above statement true when a is prime. Namely:

$$\text{If } p \text{ is a prime number and } a, b \in \mathbb{Z} \text{ such that } p|(ab) \text{ then } p|a \text{ or } p|b.$$

Let us now see why Fermat's Little Theorem is true.

Step 1: Let us first take care of the case when $a \equiv 0 \pmod{p}$. That is, when p divides a. In this case, p divides a^p as well so that both a^p and a are congruent to 0 modulo p. Therefore

$$a^p \equiv a \pmod{p}.$$

Step 2: So now suppose that a is not divisible by p. Consider

$$a, 2a, 3a, \ldots, (p-1)a.$$

Now, suppose for a minute that we had that $na \equiv ma \pmod{p}$ for some $n \neq m$ with $1 \leq m, n \leq p-1$. Remember that this means that na and ma have the same remainder when divided by p. This means that

$$na = pq_1 + r$$

and

$$ma = pq_2 + r,$$

where $q_1, q_2 \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that $0 \leq r < p$. Rearranging a bit we see that

$$(n-m)a = na - ma = pq_1 - pq_2 = p(q_1 - q_2).$$

However, this means that p divides $(n-m)a$. By the special property of prime numbers discussed above we have that $p|a$ or $p|(n-m)$. But we assumed $p \not| a$ and $n-m$ is too small to be divided by p. We must have started off on the wrong foot! Therefore each $na \not\equiv ma \pmod{p}$.

Now, we see that

$$\begin{aligned} a(2a)(3a)\cdots((p-1)a) &\equiv (p-1)(p-2)\cdots(3)(2)(1) \pmod{p} \\ &\equiv a^{p-1}(p-1)(p-2)\cdots(3)(2)(1) \pmod{p}. \end{aligned}$$

Now, another special property of prime numbers is that you can "cancel out" common nonzero numbers from each side of a congruence. Therefore we see that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplying both sides of this equation by a we see that

$$a^p \equiv a \pmod{p}.$$

This proves Fermat's theorem!

BREAK FOR PROBLEM SET

4 UPC Codes

Universal Product Codes (UPC) are assigned to items using modular arithmetic! That is, the barcodes that you see on products you buy at the store. A UPC identification number has 12 digits. The left-most and right-most digits are written smaller and in the respective corners. For example:

The first six digits identity the manufacturer and the next five digits identity the product. The last digit is called the check digit. The purpose of the check digit is to detect if a UPC code has been incorrectly entered. To explain how the check digit is calculated on a UPC code let's introduce some notation:

For two n-tuples of non-negative integers let

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = a_1b_1 + a_2b_2 + \cdots + a_nb_n.$$

An item with the UPC $a_1a_2\cdots a_{12}$ satisfies the relation

$$(a_1, a_2, \ldots, a_n) \cdot (3, 1, 3, 1, \ldots, 3, 1) \equiv 0 \pmod{10}.$$

Now, take a minute to check that the above UPC satisfies this relation. The benefit of using this relation is that it detects almost all errors made by:

- switching two adjacent numbers or
- making a mistake on one number.